memory device into a reader; the Examiner asserted, however, that the Tatebayashi et al. reference provides these teachings, and that it would have been obvious to modify the Jones et al. reference accordingly in order to authenticate the flash memory with the reader.

Applicants respectfully traverse the final rejection, and request its reconsideration.

In this regard, Applicants submit that the rejection is based, at best, on a strained reading of the Jones et al. reference. The Examiner asserted that memory array 150 of the Jones et al. reference corresponds to the flash memory device of the claim, and that smartcard integrated circuit 250 of the reference corresponds to the reader of the claim.[3] Based on this reading, the Examiner asserted that the reference teaches the inserting of a flash memory storage device into a reader because:

> flash memory are inherently inserted and removed/detached from the floppy disk driver/reader of the host computer. For instance, floppy disk which stores data, are inherently inserted and removed/detached from the floppy disk driver/reader located in the host computer.[4]

Applicants submit that this interpretation of the reference is in error, and that the stretching of this erroneous interpretation required to reach claim 1 is also in error.

First, Applicants submit that element 250 of the Jones et al. reference cannot correspond to the reader of claim 1 and its dependent claims. The Jones et al. reference clearly teaches that this element 250 (referred to as "smartcard integrated circuit 250"[5]) resides within a "Secure Memory Card"[6], and that this smart memory card is itself a PCMCIA card that is insertable and removable into the host system.[7] Accordingly, there is no reader disclosed by the Jones et al. reference whatsoever. Rather, the smart memory card 100 of the reference, which contains both memory array 150 (asserted as the flash memory storage device of claim 1) and smartcard

---

[2] U.S. Patent No. 6,859,535, issued February 22, 2005 to Tatebayashi et al., from an application filed October 15, 1999.
[3] Office Action of May 16, 2006, page 3.
[4] *Id.*
[5] Jones et al., *supra,* column 4, line 63.
[6] Jones et al., *supra,* Figure 2.
[7] Jones et al., *supra,* column 3, lines 16 through 49.

integrated circuit 250 (asserted as the reader of claim 1), is what is inserted and accessed by way of a password.

Secondly, the Examiner's assertion that "flash memory are inherently inserted and removed/detached from the floppy disk driver/reader of the host computer"[8] is nonsensical, and certainly cannot support the rejection. One first wonders how a "floppy disk driver/reader" has anything to do with a flash memory device and a flash memory reader – of course, a flash memory device is not a floppy disk. Secondly, the Jones et al. reference makes no mention whatsoever of a "floppy disk driver/reader", or even of a "floppy disk". Accordingly, it is impossible to consider how this phantom "floppy disk driver/reader" can establish the alleged inherency, when there is no mention of the "floppy disk driver/reader" in the reference itself. To the extent that the rejection is based on this alleged inherency, the rejection is therefore necessarily in error.

More fundamentally, however, Applicants submit that the Jones et al. reference simply fails to teach the inserting of a flash memory storage device into a reader, where the reader includes a memory storing a key according to which the information stored in the flash memory storage device is encrypted, as required by claim 1. In summary, it is this physical inserting step, which connotes a physical separation and separability between the flash memory storage device with the encrypted data, and the reader containing the key according to which that data is encrypted, that provides the improved security advantages in hindering unauthorized access of the key, and unauthorized access of the encrypted flash memory data without accessing the reader.[9] In contrast, to the extent that the Jones et al. reference discloses the storing of a key in smartcard integrated circuit 250, according to which the data in its memory array 150 is encrypted, the reference discloses that these two elements 150, 250 are always and forever in the same physical card, namely Secure Memory Card 100, and that this Secure Memory Card 100 is what is inserted into the host system and accessed without a reader. Accordingly, the Jones et al.

[8] Office Action, *supra,* page 3.
[9] Specification, *supra,* page 10, line 5 through page 11, line 4.

reference falls far short of the requirements of claim 1, and in fact suffers from the very problem addressed by the invention of claim 1.

The Tatebayashi et al. reference does not make up for the shortfall of the Jones et al. reference in this regard. The Examiner asserted that the Tatebayashi et al. reference adds, to the Jones et al. reference, express disclosure of the inserting of a flash memory storage device into a reader. While such inserting is in fact taught by the Tatebayashi et al. reference, the Tatebayashi et al. reference also fails to disclose that its reader stores a key according to which the information in the flash memory storage device is encrypted, or decrypted. Rather, the Tatebayashi et al. reference clearly teaches that both the encrypted contents and the key used for encrypting those contents are stored on the "recording medium device".[10] Furthermore, the Tatebayashi et al. nowhere discloses the forwarding of an access code from a host system to a reader, responsive to the validity of which, the reader obtains the key that it stores, as required by claim 1. Indeed, the "reader" of the Tatebayashi et al. reference is not connected to a host system when it decrypts and uses the decrypted information itself, considering that it is a portable audio player.[11]

Accordingly, Applicants submit that the combined teachings of the Jones et al. and Tatebayashi et al. reference fall short of the requirements of claim 1 and its dependent claims, because these combined teachings fail to disclose the storing of a key in a reader, according to which information stored on a flash memory storage device is encrypted and decrypted, as claimed. Applicants further submit that there is no suggestion from the prior art to modify these teachings in such a manner as to reach the claims. As discussed above, the method of claim 1 requires both an access code from the host system to be valid for a reader, and for the key in the reader to match the data encrypted in the insertable flash memory storage device, for the stored data to be decrypted and used. This separation of the key in the reader from the encrypted data in the storage device, in combination with the access code test applied to the communication from the host system, provides substantial security advantages over the prior art, including that

[10] Tatebayashi et al., *supra,* column 43, lines 31 through 67.
[11] Tatebayashi et al., *supra,* Figure 3.

described by the Jones et al. and Tatebayashi et al. references. In contrast, the Jones et al. reference and the Tatebayashi et al. reference both teach the storing of the key in the insertable storage device, thus failing to provide the level of security provided by the invention of claim 1 and therefore necessarily failing to suggest modifying their teachings so as to reach claim 1. Because such suggestion to modify is absent in the prior art, the application of the Jones et al. and Tatebayashi et al. references to reject claim 1 and its dependent claims under §103 is necessarily based on the improper hindsight use of Applicants' own teachings.

Reconsideration of the final rejection of claim 1 and its dependent claims 3, 5 through 8, 11, and 12 is therefore respectfully requested.

Applicants also respectfully traverse the final rejection of claim 13 and its dependent claims 17 through 22 and 24.

Independent apparatus claim 13, as before, requires a host system, a flash memory reader coupled to the host system, and means for decrypting information stored on a flash memory device received at the interface of the flash memory reader, using a key that is stored in reader memory and that is obtained by circuitry in the reader responsive to a valid access code received from the host system. The system of amended claim 13 provides similar advantages as the method of claim 1 discussed above.

Claim 13 was rejected on similar grounds as asserted against claim 1.[12] As discussed above, Applicants submit that the rejection is based on, at best, a strained reading of the Jones et al. reference and misapplication of that strained reading against the claims.

Contrary to the assertion by the Examiner, Applicants submit that element 250 of the Jones et al. reference cannot correspond to the reader of claim 1 and its dependent claims. Instead, element 250 (*i.e.,* "smartcard integrated circuit 250"[13]) of the Jones et al. reference resides within a "Secure Memory Card"[14] that is itself an insertable and removable PCMCIA

[12] Office Action, *supra,* pages 3 through 5.
[13] Jones et al., *supra,* column 4, line 63.
[14] Jones et al., *supra,* Figure 2.

card.[15] The Jones et al. reference therefore fails to disclose a flash memory reader that is coupled to a host system, and that has an interface for receiving a flash memory storage device. Rather, the entire smart memory card 100 of the Jones et al. reference, which contains both memory array 150 and smartcard integrated circuit 250, is what is inserted, and accessed by way of a password. In addition, also as discussed above relative to claim 1, Applicant submit that the Examiner's assertion that "flash memory are inherently inserted and removed/detached from the floppy disk driver/reader of the host computer"[16] does not support the rejection. The alleged "floppy disk driver/reader" has nothing to do with a flash memory device and a flash memory reader, and the Jones et al. reference makes no mention whatsoever of a "floppy disk driver/reader", or even of a "floppy disk". It is therefore impossible for this missing element from the reference to cause the reference to inherently disclose the reader of claim 13. For these reasons, Applicants submit that the final rejection of claim 13 and its dependent claims is in error.

Applicants further submit that the Jones et al. reference simply fails to teach the flash memory reader having an interface for receiving a flash memory storage device, as required by claim 13, especially such a reader that includes a memory for storing a key according to which the information stored in the flash memory storage device is decrypted by decrypting means of that reader, as required by the claim. Rather, to the extent that the Jones et al. reference discloses the storing of a key in smartcard integrated circuit 250, according to which the data in its memory array 150 is encrypted, these two elements 150, 250 are always and forever in the same physical card, namely Secure Memory Card 100. It is this Secure Memory Card 100 is what is inserted into the host system and accessed without a reader.

Nor does the Tatebayashi et al. reference provide these elements of claim 13 that are not taught by the Jones et al. reference. The Tatebayashi et al. reference fails to disclose that its reader stores a key according to which the information in the flash memory storage device is encrypted, or decrypted. Instead, the Tatebayashi et al. reference clearly teaches that both the

[15] Jones et al., *supra,* column 3, lines 16 through 49.
[16] Office Action, *supra,* page 3.

encrypted contents and the key used for encrypting those contents are stored on the "recording medium device".[17] Furthermore, the Tatebayashi et al. nowhere discloses means for receiving an access code from a host system, nor means for obtaining the key stored in the reader memory responsive to this access code being valid, as required by the reader of claim 13. In fact, the "reader" of the Tatebayashi et al. reference does not operate with a host system when it decrypts and uses the decrypted information itself, considering that it is a portable audio player.[18]

Accordingly, Applicants submit that the combined teachings of the Jones et al. and Tatebayashi et al. reference also fall short of the requirements of claim 13 and its dependent claims, because these combined teachings fail to disclose a flash memory reader including an interface for receiving a flash memory device, including a reader memory for storing a key according to which information is decrypted by decrypting means in the reader, and also including the accessing circuitry including means for receiving an access code from the host system, all as recited in claim 13. Nor is there suggestion from the prior art to modify these teachings in such a manner as to reach the claims, considering that neither reference discloses a system in which the flash memory data is decrypted responsive to both a valid access code being received from the host system and also the key stored in the reader matching the data encrypted in the insertable flash memory storage device. It is this separation of the key in the reader from the encrypted data in the storage device, in combination with the access code test applied to the communication from the host system, that provides the substantial security advantages over the prior art, including that described by the Jones et al. and Tatebayashi et al. references. Absent such suggestion to modify, the rejection of claim 13 and its dependent claims is necessarily based on the improper hindsight use of Applicants' own teachings.

Reconsideration of the final rejection of claim 1 and its dependent claims 17 through 22 and 24 is therefore respectfully requested.

The prior art cited as pertinent but not applied has been considered, but is not felt to come within the scope of the claims in this case.

---

[17] Tatebayashi et al., *supra,* column 43, lines 31 through 67.
[18] Tatebayashi et al., *supra,* Figure 3.

For these reasons, Applicants respectfully submit that all claims now in this case are in condition for allowance. Reconsideration of this application is therefore respectfully requested.

Respectfully submitted,
/Rodney M. Anderson/
Rodney M. Anderson
Registry No. 31,939
Attorney for Applicants

Anderson, Levine & Lintel, L.L.P.
14785 Preston Road, Suite 650
Dallas, Texas 75254
(972) 664-9554